

# Divisibility questions in abelian varieties

Laura Paladino\*

## Abstract

Let  $k$  be a number field, with algebraic closure  $\bar{k}$ , and let  $\mathcal{A}$  be an abelian variety over  $k$  of dimension  $n = 2^h$ , where  $h \geq 0$ . Let  $p$  be a prime number and let  $\mathcal{A}[p]$  denote the  $p$ -torsion subgroup of  $\mathcal{A}$ . We prove that for every  $h$ , there exists a prime  $p_h$ , depending only on  $h$ , such that if  $\mathcal{A}[p]$  is either an irreducible or a decomposable  $\text{Gal}(\bar{k}/k)$ -module, then for all primes  $p > p_h$  the local-global divisibility by  $p$  holds in  $\mathcal{A}(k)$  and  $\text{III}^1(k, \mathcal{A}[p])$  is trivial. In particular, when  $\mathcal{A}$  has dimension 2 or 4, we show  $p_h = 3$ . This result generalizes some previous ones proved for elliptic curves. In the case when  $\mathcal{A}$  is principally polarized, the vanishing of  $\text{III}^1(k, \mathcal{A}[p])$  implies that the elements of the Tate-Shafarevich group  $\text{III}(k, \mathcal{A})$  are divisible by  $p$  in the Weil-Châtelet group  $H^1(k, \mathcal{A})$  and the local-global principle for divisibility by  $p$  holds in  $H^r(k, \mathcal{A})$ , for all  $r \geq 0$ .

## 1 Introduction

We consider two local-global problems, strongly related, that recently arose as generalizations of some classical questions. The setting is the one of an abelian variety  $\mathcal{A}$  of dimension  $g$  defined over number field  $k$ . Let  $\bar{k}$  be the algebraic closure of  $k$  and let  $M_k$  be the set of places  $v$  of  $k$ . For every positive integer  $q$ , we denote by  $\mathcal{A}[q]$  be the  $q$ -torsion subgroup of  $\mathcal{A}$  and by  $k(\mathcal{A}[q])$  the number field obtained by adding to  $k$  the coordinates of the  $q$ -torsion points of  $\mathcal{A}$ . It is well-known that  $\mathcal{A}[q] \simeq (\mathbb{Z}/q\mathbb{Z})^{2g}$  and that the Galois group  $\text{Gal}(k(\mathcal{A}[q])/k)$  is isomorphic to the image of the representation of the absolute Galois group  $\text{Gal}(\bar{k}/k)$  in the general linear group  $\text{GL}_{2g}(\mathbb{Z}/q\mathbb{Z})$ . The behaviour of  $\text{Gal}(k(\mathcal{A}[q])/k)$  is related to the answer of the following question, known as *Local-global divisibility problem*.

---

\*Partially supported by Istituto Nazionale di Alta Matematica F. Saveri with grant “Assegno di ricerca Ing. Giorgio Schirillo”

**Problem 1.** *Let  $P \in \mathcal{A}(k)$  and let  $q$  be a positive integer. Assume that for all but finitely many valuations  $v \in k$ , there exists  $D_v \in \mathcal{A}(k_v)$  such that  $P = qD_v$ . Is it possible to conclude that there exists  $D \in \mathcal{A}(k)$  such that  $P = qD$ ?*

This problem was stated in 2001 by Dvornicich and Zannier in the more general case when  $\mathcal{A}$  is a commutative algebraic group and its formulation was motivated by a particular case of the famous Hasse Principle on quadratic forms and by the Grunwald-Wang Theorem (see [9] and [10]). The vanishing of the first cohomology group  $H^1(\text{Gal}(k(\mathcal{A}[q])/k), \mathcal{A}[q])$  assures a positive answer (see for instance [9], [23]). Clearly a solution to Problem 1 for all powers  $p^l$  of prime numbers  $p$  is sufficient to get an answer for all integers  $q$ , by the unique factorization in  $\mathbb{Z}$  and Bézout's identity.

In the case of elliptic curves the problem has been widely studied since 2001 and recently a complete answer has been proved when  $k = \mathbb{Q}$ . The answer is affirmative when  $q$  is a prime  $p$  (see [9], [23]) and for powers  $p^l$ , where  $p \geq 5$  and  $l \geq 2$  (see [21]). On the contrary, the answer is negative for  $q = p^l$ , with  $p \in \{2, 3\}$  and  $l \geq 2$  (see [7], [10], [17], [19]). For a general number field  $k$ , the answer is still positive when  $q$  is a prime  $p$  (see [9], [23]). With a mild hypothesis on  $k$ , the proof of [11, Theorem 1] implies the following statement (see also [20]).

**Theorem 1.1.** *Let  $p$  be a prime. Let  $\mathcal{E}$  be an elliptic curve defined over a number field  $k$  which does not contain the field  $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ , where  $\zeta_p$  is a primitive  $p$ th root of the unity. If  $\mathcal{E}$  does not admit any  $k$ -rational isogeny of degree  $p$ , then the local-global principle holds for divisibility by  $p^l$  in  $\mathcal{E}$  over  $k$ , for every positive integer  $l$ .*

The hypothesis that  $k$  does not contain  $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$  is necessary (see [21, Sec. 6]). Stronger criteria for the local-global divisibility in elliptic curves have been given in [20] and [21]. In particular there exists a prime  $p_k$ , depending only on  $k$ , such that if  $p > p_k$  then the answer is positive for divisibility by  $p^l$ , for all  $l \geq 1$ . Here we prove the following statements that assures the local-global divisibility by  $p$  on some abelian varieties of higher dimension satisfying certain conditions.

**Theorem 1.2.** *Let  $p$  be a prime number. Let  $k$  be a number field that does not contain  $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ . Let  $\mathcal{A}$  be an abelian variety defined over  $k$ , of dimension  $n = 2^h$ , where  $h \geq 0$ . For every  $h$ , there exists a prime  $p_h$ , depending only on  $h$ , such that if  $\mathcal{A}[p]$  is either an irreducible or a decomposable  $\text{Gal}(\bar{k}/k)$ -module, then the local-global divisibility*

by  $p$  holds in  $\mathcal{A}(k)$ , for all  $p \geq p_h$ . In particular, for abelian varieties of dimension 2 and 4, we have  $p_1 = p_2 = 3$ .

Evidently, Theorem 1.2 implies the following result that reminds of Theorem 1.1 for divisibility by  $p$  in higher dimension.

**Corollary 1.3.** *Let  $p$  be a prime number. Let  $k$  be a number field that does not contain  $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ . Let  $\mathcal{A}$  be an abelian variety defined over  $k$ , of dimension  $n = 2^h$ , where  $h \geq 0$ . For every  $h$ , there exists a prime  $p_h$ , depending only on  $h$ , such that if  $\mathcal{A}$  does not admit a  $k$ -rational isogeny of degree  $p^\alpha$ , with  $1 \leq \alpha \leq 2n - 1$ , then the local-global divisibility by  $p$  holds in  $\mathcal{A}(k)$ , for all  $p \geq p_h$ . In particular, for abelian varieties of dimension 2 and 4, we have  $p_1 = p_2 = 3$ .*

Both Theorem 1.2 and its direct consequence Corollary 1.3 follow immediately by the proof of the next statement.

**Theorem 1.4.** *Let  $p$  be a prime number and let  $l, m$  be positive integers. Let  $k$  be a number field that does not contain  $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ . Let  $\mathcal{A}$  be an abelian variety defined over  $k$ , of dimension  $2^h$ , where  $h \geq 0$ . Let  $n = 2^{h+1}$  and assume that  $\text{Gal}(k(\mathcal{A}[p^l])/k)$  is isomorphic to a subgroup of  $\text{GL}_n(p^m)$ , for some positive integer  $m$ . For every  $h$ , there exists a prime  $p_h$ , depending only on  $h$ , such that if  $p > p_h$  and the local-global divisibility by  $p$  fails in  $\mathcal{A}(k)$ , then  $\text{Gal}(k(\mathcal{A}[p^l])/k)$  acts reducibly but not decomposably over  $\mathcal{A}[p^l]$ . In particular, for abelian varieties of dimension 2 and 4, we have  $p_1 = p_2 = 3$ .*

Our proof of Theorem 1.4 shows that the Tate-Shafarevich group  $\text{III}^1(k, \mathcal{A}[p])$  is trivial when  $\mathcal{A}[p]$  is either an irreducible or a decomposable  $\text{Gal}(\bar{k}/k)$ -module and  $p > p_h$ . If  $\mathcal{A}$  is principally polarized, then the triviality of  $\text{III}^1(k, \mathcal{A})$  implies  $\text{III}(k, \mathcal{A}) \subseteq pH^r(k, \mathcal{A})$ , for all  $r \geq 0$ , by [8, Theorem 2.1]. In that case we have an affirmative answer to the following second and more general problem, for all  $r$ .

**Problem 2.** *Let  $q$  be a positive integer and let  $\sigma \in H^r(k, \mathcal{A})$ . Assume that for all  $v \in M_k$  there exists  $\tau_v \in H^r(k_v, \mathcal{A})$  such that  $q\tau_v = \sigma$ . Can we conclude that there exists  $\tau \in H^r(k, \mathcal{A})$ , such that  $q\tau = \sigma$ ?*

Problem 2 was firstly considered by Cassel for  $r = 1$  in the case when  $\mathcal{A}$  is an elliptic curve  $\mathcal{E}$  (see [4, Problem 1.3]). In particular Cassels questioned if the elements of the Tate-Shafarevich group  $\text{III}(k, \mathcal{E})$  were divisible by  $p^l$  in the Weil-Châtelet group  $H^1(k, \mathcal{E})$ , for all  $l$ . Tate produced an affirmative answer for divisibility by  $p$ , but the question for

powers  $p^l$ , with  $l \geq 2$  remained open (see [5]). The mentioned results to Problem 1 imply an answer to Problem 2 too, since the proofs show the triviality or the non triviality of the corresponding Tate-Shafarevich group. So Cassel's question has an affirmative answer for  $p \geq 5$  and a negative one for  $p \in \{2, 3\}$  in elliptic curves. The problem was afterwards considered for abelian varieties by Bařmakov (see [2]) and lately by Ćiperiani and Stix, who gave some sufficient conditions for a positive answer (see [6]). In [7] Creutz proved that for every prime  $p$ , there exist infinitely many non-isomorphic abelian varieties  $A$  defined over  $\mathbb{Q}$  such that  $\text{III}(k, A) \not\subseteq pH^1(k, A)$ . In abelian varieties of dimension strictly greater than 1, even the local-global divisibility by  $p$  may fail for both Problem 1 and Problem 2 (see also [9, §3]). Here we prove the following statement.

**Theorem 1.5.** *Let  $p$  be a prime number. Let  $k$  be a number field that does not contain  $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ . Let  $\mathcal{A}$  be a principally polarized abelian variety defined over  $k$ , of dimension  $2^h$ , where  $h \geq 0$ . There exists a prime  $p_h$ , depending only on  $h$ , such that if the  $p$ -torsion subgroup  $\mathcal{A}[p]$  of  $\mathcal{A}$  is either an irreducible or a decomposable  $\text{Gal}(\bar{k}/k)$ -module, then the elements of  $\text{III}(k, \mathcal{A})$  are divisible by  $p$  in the Weil-Châtelet group  $H^1(k, \mathcal{A})$ , i. e.  $\text{III}(k, \mathcal{A}) \subseteq pH^1(k, \mathcal{A})$ , for all  $p > p_h$ . In particular for abelian varieties of dimension 2 and 4 we have  $p_h = 3$ .*

As mentioned above, the conclusion of Theorem 1.5 assures an affirmative answer to Problem 2, for all  $r \geq 0$ , in the case when  $\mathcal{A}$  is abelian variety satisfying the hypotheses of the statement and  $p > p_h$ . Then, for such abelian varieties and  $p > p_h$ , we have a local-global principle for divisibility by  $p$  in  $H^r(K, \mathcal{A})$ , for all  $r$ . The result is particularly interesting for abelian varieties of dimension 2 or 4, since we have an explicit  $p_h = 3$ .

A few preliminary results in the theory of groups and in local-global divisibility are stated in next section. In Section 2 we treat the special case in which  $\text{Gal}(k(\mathcal{A}[p^l])/k)$  acts decomposably over  $k(\mathcal{A}[p^l])$ , in particular when  $\mathcal{A}$  is a product of elliptic curves. In the last and main part of the paper, we proceed with the proof of Theorem 1.4.

## 2 Preliminary results

We recall some known results about local-global divisibility and about group theory, that will be useful for the proof of Theorem 1.4.

As above, let  $k$  be a number field and let  $\mathcal{A}$  be an abelian variety of dimension  $g$ , defined over  $k$ . Let  $q := p^l$ , where  $p$  is a prime number and  $l$  is a positive integer. As

introduced before, the  $p^l$ -torsion subgroup of  $\mathcal{A}$  will be denoted by  $\mathcal{A}[p^l]$  and the number field obtained by adding to  $k$  the coordinates of the points in  $\mathcal{A}[p^l]$  will be denoted by  $F := k(\mathcal{A}[p^l])$ . The  $p$ -torsion subgroup  $\mathcal{A}[p]$  of  $\mathcal{A}$  is a  $G_k$ -module, where  $G_k$  denotes the absolute Galois group  $\text{Gal}(\bar{k}/k)$ . Since  $\mathcal{A}[p] \simeq (\mathbb{Z}/p\mathbb{Z})^n$ , with  $n = 2g$ , then  $G_k$  acts over  $\mathcal{A}[p]$  as a subgroup of  $\text{GL}_n(\mathbb{Z}/p\mathbb{Z})$  isomorphic to  $G := \text{Gal}(k(\mathcal{A}[p])/k)$ . We still denote by  $G$  the representation of  $G_k$  in  $\text{GL}_n(\mathbb{Z}/p\mathbb{Z})$ . If  $l = 1$ , in particular  $G \leq \text{GL}_n(p)$ .

Let  $\Sigma$  be a subset of  $M_k$  containing all but finitely many places  $v$ , such that  $v \notin \Sigma$ , for all  $v$  ramified in  $F$ . For every  $v \in \Sigma$ , we denote by  $G_v$  the Galois group  $\text{Gal}(F_w/k_v)$ , where  $w$  is a place of  $F$  extending  $v$ . In [9] Dvornicich and Zannier proved that the answer to the local-global question for divisibility by  $q$  of points in  $\mathcal{A}(k)$  is linked to the behaviour of the following subgroup of  $H^1(G, \mathcal{A}[q])$

$$H_{\text{loc}}^1(G, \mathcal{A}[q]) := \bigcap_{v \in \Sigma} \ker H^1(G, \mathcal{A}[q]) \xrightarrow{\text{res}_v} H^1(G_v, \mathcal{A}[q]), \quad (2.1)$$

where  $\text{res}_v$ , as usual, denotes the restriction map. By substituting  $M_k$  to  $\Sigma$  in (2.1), i. e. by letting  $v$  vary over all the valuations of  $k$ , we get the classical definition of the Tate-Shafarevich group  $\text{III}^1(k, \mathcal{A}[q])$  (up to isomorphism)

$$\text{III}^1(k, \mathcal{A}[q]) := \bigcap_{v \in M_k} \ker H^1(k, \mathcal{A}[q]) \xrightarrow{\text{res}_v} H^1(k_v, \mathcal{A}[q]).$$

In particular, the vanishing of  $H_{\text{loc}}^1(G, \mathcal{A}[q])$  assures the triviality of  $\text{III}^1(k, \mathcal{A}[q])$ , that is a sufficient condition to get an affirmative answer to Problem 2, for all  $r \geq 0$ , in the case when  $\mathcal{A}$  is principally polarized (see [8, Theorem 2.1]). Furthermore the vanishing of  $H_{\text{loc}}^1(G, \mathcal{A}[q])$  is a sufficient condition for an affirmative answer to Problem 1 (see [9, Proposition 2.1]).

Because of Čebotarev's Density Theorem, the group  $G_v$  varies over all cyclic subgroups of  $G$  as  $v$  varies in  $\Sigma$ , then in [9] Dvornicich and Zannier gave the following equivalent definition of  $H_{\text{loc}}^1(G, \mathcal{A}[q])$ .

**Definition 2.1.** A cocycle  $\{Z_\sigma\}_{\sigma \in G} \in H^1(G, \mathcal{A}[q])$  satisfies the local conditions if, for every  $\sigma \in G$ , there exists  $A_\sigma \in \mathcal{A}[q]$  such that  $Z_\sigma = (\sigma - 1)A_\sigma$ . The subgroup of  $H^1(G, \mathcal{A}[q])$  formed by all the cocycles satisfying the local conditions is called *first local cohomological group* of  $G$  with values in  $\mathcal{A}[q]$  and it is denoted by  $H_{\text{loc}}^1(G, \mathcal{A}[q])$ .

The description of  $H_{\text{loc}}^1(G, \mathcal{A}[q])$  given in Definition 2.1 is useful in proving its triviality and even in producing counterexamples to the local-global divisibility. We keep the notation  $H_{\text{loc}}^1(G, \mathcal{A}[q])$  used in almost all previous papers about the topic, but it is worth to mention that in [22] Sansuc already treated similar modified Tate-Shafarevich groups as in (2.1) and introduced the notation  $\text{III}_{\Sigma}^1(k, \mathcal{A})$ .

The vanishing of  $H_{\text{loc}}^1(G, \mathcal{A}[p^l])$  is strongly related to the behaviour of  $H_{\text{loc}}^1(G_p, \mathcal{A}[p^l])$ , where  $G_p$  is the  $p$ -Sylow subgroup of  $G$  (see [9]).

**Lemma 2.2** (Dvornicich, Zannier). *Let  $G_p$  be the  $p$ -Sylow subgroup of  $A$ . An element of  $H_{\text{loc}}^1(\mathcal{A}, \mathcal{A}[p^l])$  is zero if and only if its restriction to  $H_{\text{loc}}^1(G_p, \mathcal{A}[p^l])$  is zero.*

In some cases, a quick way to show that both  $H_{\text{loc}}^1(G, \mathcal{A}[p^l])$  and  $H_{\text{loc}}^1(G_p, \mathcal{A}[p^l])$  are trivial is the use of Sah's Theorem (see [15, Theorem 5.1]).

**Lemma 2.3** (Sah's Theorem). *Let  $G$  be a group and let  $M$  be a  $G$ -module. Let  $\alpha$  be in the center of  $G$ . Then  $H^1(G, M)$  is annihilated by the map  $x \rightarrow \alpha x - x$  on  $M$ . In particular, if this map is an automorphism of  $M$ , then  $H^1(G, M) = 0$ .*

By Lemma 2.3, if  $G$  is a subgroup of  $\text{GL}_n(p^l)$  that contains a non-trivial scalar matrix, then  $H^1(G, \mathbb{Z}/q\mathbb{Z}) = 0$ . Thus, in particular, the same holds for  $H_{\text{loc}}^1(G, \mathcal{A}[q]) = 0$ .

**Corollary 2.4.** *Let  $G \leq \text{GL}_n(q)$ , for some positive integers  $n$  and  $q$ . If  $\lambda \cdot I_n \in G$  is a nontrivial scalar matrix, then  $H_{\text{loc}}^1(G, \mathcal{A}[q]) = 0$ .*

In our proof of Theorem 1.4, a crucial tool is the use of Aschbacher's Theorem on the classification of maximal subgroups of  $\text{GL}_n(q)$  (see [1]). Aschbacher proved that the maximal subgroups of  $\text{GL}_n(q)$  could be divided into 9 specific classes  $\mathcal{C}_i$ ,  $1 \leq i \leq 9$ . For a big  $n$ , it is a very hard open problem to find the maximal subgroups of  $\text{GL}_n(q)$  of type  $\mathcal{C}_9$ . We have an explicit list of such groups only for  $n \leq 12$  (see [3]). On the contrary, the maximal subgroups of  $\text{GL}_n(q)$  of geometric type (i. e. of class  $\mathcal{C}_i$ , with  $1 \leq i \leq 8$ ) have been described for every  $n$  (see [14]). We recall some notations in group theory and then we resume the description of the maximal subgroups of geometric type in the following Table 1 (see [14, Table 1.2.A and § 3.5]).

**Notation 1.** Let  $n, q$  be positive integers and let  $\mathbb{F}_q$  be the finite field with  $q$  elements. Let  $\omega_q$  be a primitive element of  $\mathbb{F}_q^*$ . We use the standard notations for the special linear group  $\text{SL}_n(q)$ , the projective special linear group  $\text{PSL}_n(q)$ , the special orthogonal group

$\mathrm{SO}_n(q)$ , the unitary group  $\mathrm{U}_n(q)$ , the symplectic group  $\mathrm{Sp}_n(q)$ , the symmetric group  $S_n$  and the alternating group  $A_n$ . By  $C_n$  we denote a cyclic group of order  $n$ , by  $E_n$  an elementary abelian group of order  $n$  and by  $p^{1+2n}$  an extraspecial group of order  $p^{1+2n}$ . Furthermore, if  $n$  is even and  $q$  is odd we denote by (see [3])

$\mathrm{GO}_n^+(q)$  the stabilizer of the non-degenerate symmetric bilinear antidiagonal form  $(1, \dots, 1)$ ;

$\mathrm{SO}_n^+(q)$  the subgroup of  $\mathrm{GO}_n^+(q)$  formed by the matrices with determinant 1;

$\mathrm{GO}_n^-(q)$  the stabilizer of non-degenerate symmetric bilinear form  $I_n$ , when  $n \equiv 2 \pmod{4}$  and  $q \equiv 3 \pmod{4}$  and the stabilizer of non-degenerate symmetric bilinear diagonal form  $(\omega_q, 1, \dots, 1)$ , when  $n \not\equiv 2 \pmod{4}$  and  $q \not\equiv 3 \pmod{4}$ ;

$\mathrm{SO}_n^-(q)$  the subgroup of  $\mathrm{GO}_n^-(q)$  formed by the matrices with determinant 1.

**Notation 2.** Let  $A, B$  be two groups. We denote by

$A \rtimes B$ , the semidirect product of  $A$  with  $B$  (where  $A \trianglelefteq A \rtimes B$ );

$A \circ B$ , the central product of  $A$  and  $B$ ;

$A \wr B$ , the wreath product of  $A$  and  $B$ ;

$A.B$ , a group  $\Gamma$  that is an extension of its normal subgroup  $A$  with the group  $B$  (then  $B \simeq \Gamma/A$ ), in the case when we do not know if it is a split extension or not;

$A \cdot B$ , a group  $\Gamma$  that is a non-split extension of its normal subgroup  $A$  with the group  $B$  (then  $B \simeq \Gamma/A$ );

$A : B$ , a group  $\Gamma$  that is a split extension of its normal subgroup  $A$  with the group  $B$  (then  $B \simeq \Gamma/A$  and  $\Gamma \simeq A \rtimes B$ ).

type	description	structure
$\mathcal{C}_1$	stabilizers of a totally singular or nonsingular subspace	maximal parabolic group
$\mathcal{C}_2$	stabilizers of a direct sum decomposition $V = \bigoplus_{i=1}^r V_i$ , with each $V_i$ of dimension $t$	$\mathrm{GL}_t(q) \wr S_r, n = rt$
$\mathcal{C}_3$	stabilizers of an extension field of $\mathbb{F}_q$ of prime index $r$	$\mathrm{GL}_t(q^r).C_r, n = rt, r$ prime
$\mathcal{C}_4$	stabilizers of tensor product decomposition $V = V_1 \otimes V_2$	$\mathrm{GL}_t(q) \circ \mathrm{GL}_r(q), n = rt$
$\mathcal{C}_5$	stabilizers of subfields of $\mathbb{F}_q$ of prime index $r$	$\mathrm{GL}_n(q_0), q = q_0^r, r$ prime
$\mathcal{C}_6$	normalizers of symplectic-type $r$ -groups ( $r$ prime) in absolutely irreducible representations	$E_{r^{2t}}.\mathrm{Sp}_{2t}(r), n = r^t, r$ prime $2^{1+2t}.\mathrm{O}_{2t}^-(r), n = 2^t$ $2_+^{1+2t}.\mathrm{O}_{2t}^+(r), n = 2^t$
$\mathcal{C}_7$	stabilizers of decompositions $V = \bigotimes_{i=1}^t V_i, \dim(V_i) = r$	$\underbrace{(\mathrm{GL}_r(q) \circ \dots \circ \mathrm{GL}_r(q))}_t.S_r, n = r^t$
$\mathcal{C}_8$	classical subgroups	$\mathrm{Sp}_n(q), n$ even $\mathrm{O}_n^\epsilon(q), q$ odd $\mathrm{U}_n(q^{\frac{1}{2}}), q$ a square

Table 1: Maximal subgroups of  $\mathrm{GL}_n(q)$  of geometric types

Although we generally do not know explicitly the maximal subgroups of type  $\mathcal{C}_9$ , by Aschbacher's Theorem, we have such a characterization of them:

“if  $\Gamma$  is a maximal subgroup of  $\mathrm{GL}_n(q)$  of class  $\mathcal{C}_9$  and  $Z$  denotes its center, then for some nonabelian simple group  $T$ , the group  $\Gamma/(\Gamma \cap Z)$  is almost simple with socle  $T$ ; in this case the normal subgroup  $(\Gamma Z).T$  acts absolutely irreducibly, preserves no nondegenerate classical form, is not a subfield group, and does not contain  $\mathrm{SL}_n(q)$ .”

For very small integers  $n$  there are a few subsequent and more explicit versions of Aschbacher's Theorem, that describe explicitly the subgroups of class  $\mathcal{C}_9$ . To prove Theorem 1.3 we will use the classification of the maximal subgroups of  $\mathrm{SL}_n(q)$  appearing in [3], for  $n \in \{4, 8\}$ .

### 3 Decomposable actions and products of elliptic curves

First of all we investigate what happens when the group  $G = \mathrm{Gal}(k(\mathcal{A}[q])/k, \mathcal{A}[q])$  acts decomposably on  $\mathcal{A}[q]$ , i. e., the representation of  $G_k$  in  $\mathrm{GL}_n(q)$  is a group of matrices with diagonal blocks. For instance, this is the case when  $\mathcal{A}$  is a direct product of elliptic curves.



**Lemma 3.1.** *Let  $q$  be a positive integer. Suppose that  $G$  acts decomposably on  $\mathcal{A}[q]$ , i. e. the representation of  $G$  in  $\mathrm{GL}_n(\mathbb{Z}/q\mathbb{Z})$  is of the form*

$$\begin{pmatrix} B_1 & 0 & \dots & & 0 \\ 0 & B_2 & 0 & \dots & 0 \\ \vdots & & \ddots & & \vdots \\ & & & \ddots & 0 \\ 0 & \dots & & 0 & B_s \end{pmatrix} \quad (3.1)$$

where  $B_i \in \mathrm{GL}_{n_i}$ , for  $i \in \{1, 2, \dots, s\}$  and  $\sum_{i=1}^s n_i = n$ . Let  $G_i$  denote the subgroup of  $\mathrm{GL}_{n_i}$  formed by the matrices  $B_i$ , for all  $1 \leq i \leq s$ . Then  $H_{\mathrm{loc}}^1(G, \mathbb{Z}/q\mathbb{Z}^n) = 0$  if and only if  $H_{\mathrm{loc}}^1(G_i, \mathbb{Z}/q\mathbb{Z}^{n_i}) = 0$ , for all  $1 \leq i \leq s$ .

*Proof.* The conclusion is a direct consequence of  $H^1(G, -)$  being an additive functor and  $H_{\mathrm{loc}}^1(G, -)$  being a subfunctor of his (see for instance [12] and [13]); anyway we show a proof involving local cocycles. We prove the statement when  $s = 2$ . When  $s > 2$ , the conclusion follows by induction. Assume that the representation of  $G = \mathrm{Gal}(k(\mathcal{A}[q])/k, \mathcal{A}[q])$  in  $\mathrm{GL}_n(\mathbb{Z}/q\mathbb{Z})$  is of the form

$$\begin{pmatrix} B_1 & 0 \\ 0 & B_2 \end{pmatrix},$$

where  $B_1 \in \mathrm{GL}_{n_1}(\mathbb{Z}/q\mathbb{Z})$ ,  $B_2 \in \mathrm{GL}_{n-n_1}(\mathbb{Z}/q\mathbb{Z})$ . Of course  $G_1$  and  $G_2$  can be identified with subgroups of  $G$ . If a cocycle of  $G$  satisfies the local conditions, in particular its restriction to any subgroup of  $G$  satisfies the local conditions too. Thus  $H_{\mathrm{loc}}^1(G, \mathbb{Z}/q\mathbb{Z}^n) = 0$  implies  $H_{\mathrm{loc}}^1(G_i, \mathbb{Z}/q\mathbb{Z}^{n_i}) = 0$ , for  $i \in \{1, 2\}$ . Let  $\{a_{i,j}\}_{1 \leq i,j \leq n}$  denote a matrix in  $G$ ; consequently  $\{a_{i,j}\}_{1 \leq i,j \leq n_1}$  and  $\{a_{i,j}\}_{n_1+1 \leq i,j \leq n}$  are matrices in  $G_1$  and  $G_2$ , respectively. Suppose that there exists a cocycle  $\{Z_\sigma\}_{\sigma \in G}$  of  $G$  with values in  $(\mathbb{Z}/q\mathbb{Z})^n$  satisfying the local conditions, with  $Z_\sigma = (z_{\sigma,1}, \dots, z_{\sigma,n})$ . We define two new cocycles, one of  $G_1$  with values in  $(\mathbb{Z}/q\mathbb{Z})^{n_1}$  and the other of  $G_2$  with values in  $(\mathbb{Z}/q\mathbb{Z})^{n-n_1}$ , respectively by  $Z_{\sigma, B_1} := (z_{\sigma,1}, \dots, z_{\sigma,n_1}) \in (\mathbb{Z}/q\mathbb{Z})^{n_1}$  and  $Z_{\sigma, B_2} := (z_{\sigma,n_1+1}, \dots, z_{\sigma,n}) \in (\mathbb{Z}/q\mathbb{Z})^{n-n_1}$ . Since  $\{Z_\sigma\}_{\sigma \in G}$  satisfies the local conditions, then  $\{Z_{\sigma, B_1}\}_{B_1 \in G_1}$  and  $\{Z_{\sigma, B_2}\}_{B_2 \in G_2}$  satisfy the local conditions too. Because of our hypothesis that  $H_{\mathrm{loc}}^1(G_1, (\mathbb{Z}/q\mathbb{Z})^{n_1}) = 0$ , there exists  $W_1 = (w_1, \dots, w_{n_1}) \in (\mathbb{Z}/q\mathbb{Z})^{n_1}$ , such that  $(B_1 - I_{n_1})W_1 = Z_{\sigma, B_1}$ , for all  $B_1 \in G_1$ . In the same way, since  $H_{\mathrm{loc}}^1(G_2, (\mathbb{Z}/q\mathbb{Z})^{n-n_1}) = 0$ , then there exists  $W_2 = (w_{n_1+1}, \dots, w_n) \in (\mathbb{Z}/q\mathbb{Z})^{n-n_1}$ , such that  $(B_2 - I_{n-n_1})W_2 = Z_{\sigma, B_2}$ , for all  $B_2 \in G_2$ . Let  $W = (w_1, \dots, w_{n_1}, w_{n_1+1}, \dots, w_n) \in (\mathbb{Z}/q\mathbb{Z})^n$ . Therefore  $(G - I_n)W = Z_\sigma$ , for all

$\sigma \in G$ . We have proved that every cocycle of  $G$  with values in  $(\mathbb{Z}/q\mathbb{Z})^n$  and satisfying the local conditions is a coboundary; thus  $H_{\text{loc}}^1(G, (\mathbb{Z}/q\mathbb{Z})^n) = 0$ .  $\square$

**Remark 3.2.** Observe that the conclusion of Lemma 3.1 holds even if we suppose that the image of the representation of  $\text{Gal}(k(\mathcal{A}[q])/k)$  in  $\text{GL}_n(\mathbb{Z}/q\mathbb{Z})$  is isomorphic to a subgroup of  $\text{GL}_n(p^m)$  (for some prime  $p$  and some positive integer  $m$ ). We have such a technical assumption in the statement of Theorem 1.4.

With Lemma 3.1 and a known answer to the problem for elliptic curves, the case of products of elliptic curves is quite obvious to solve. Anyway it is worth to be mentioned here for completeness.

**Theorem 3.3.** *Let  $k$  be a number field and let  $\mathcal{E}_1, \mathcal{E}_2$  be elliptic curves with Weierstrass form respectively  $y^2 = x^3 + b_i x + c_i$ , for  $i \in \{1, 2\}$ , where  $b_i, c_i \in k$ . Let  $p$  be a prime number and  $l$  be a positive integer. The local-global divisibility by  $p^l$  holds in the product  $\mathcal{E}_1 \times \mathcal{E}_2$  over  $k$  if and only if it holds in both  $\mathcal{E}_1$  over  $k$  and  $\mathcal{E}_2$  over  $k$ .*

*Proof.* To ease notation let  $\mathcal{A} = \mathcal{E}_1 \times \mathcal{E}_2$ . The fundamental observation is that the representation of the Galois group  $\text{Gal}(k(\mathcal{A}[p^l])/k)$  in  $\text{GL}_4(\mathbb{Z}/p^l\mathbb{Z})$  is a group of matrices with two diagonal blocks (each of them with 2 rows and 2 columns). It is not true in general that the whole automorphism group of a product of elliptic curves is formed by matrices with diagonal blocks. Anyway, this is the exact situation when we restrict to automorphisms corresponding to actions of  $\text{Gal}(k(\mathcal{A}[p^l])/k)$ . In fact, every automorphism of  $\mathcal{A}$  in  $\text{Gal}(k(\mathcal{A}[p^l])/k)$  corresponds to a Galois homomorphism of the extension  $k(\mathcal{A}[p^l])/k$ , whose action on the points of  $\mathcal{A}$  can be viewed as two separate actions on the points of  $\mathcal{E}_1$  and  $\mathcal{E}_2$  (even when  $\mathcal{E}_1 = \mathcal{E}_2$ ). We can apply Lemma 3.1 to get the conclusion.  $\square$

The argument in the previous proof works also if we have an abelian variety of dimension  $g$ , that is the product of elliptic curves  $\mathcal{E}_1, \dots, \mathcal{E}_g$  satisfying the hypotheses of Theorem 3.3. Then, more generally, we have the following statement.

**Theorem 3.4.** *Let  $k$  be a number field, let  $g$  be a positive integer and let  $\mathcal{E}_1, \mathcal{E}_2, \dots, \mathcal{E}_g$  be elliptic curves with Weierstrass form respectively  $y^2 = x^3 + b_i x + c_i$ , for  $i \in \{1, 2, \dots, g\}$ , where  $b_i, c_i \in k$ . Let  $p$  be a prime number and  $l$  be a positive integer. The local-global divisibility by  $p^l$  holds in the product  $\mathcal{E}_1 \times \mathcal{E}_2 \dots \times \mathcal{E}_g$  over  $k$  if and only if it holds in every curve  $\mathcal{E}_i$ , over  $k$ , for all  $1 \leq i \leq g$ .*

By using Theorem 3.4 and [20, Corollary 2], we get the next result.

**Corollary 3.5.** *Let  $k$  be a number field, let  $g$  be a positive integer and let  $\mathcal{E}_1, \mathcal{E}_2, \dots, \mathcal{E}_g$  be elliptic curves with Weierstrass form respectively  $y^2 = x^3 + b_i x + c_i$ , for  $i \in \{1, 2, \dots, g\}$ , where  $b_i, c_i \in k$ . Let  $p$  be a prime number. Then there exists a number  $C([k : \mathbb{Q}])$  depending only on the degree  $[k : \mathbb{Q}]$ , such that, if  $p > C([k : \mathbb{Q}])$ , then the local-global divisibility by  $p^l$  holds in the product  $\mathcal{E}_1 \times \mathcal{E}_2 \dots \times \mathcal{E}_g$  over  $k$ , for every positive integer  $l$ .*

Furthermore, if  $k = \mathbb{Q}$ , we can combine Theorem 3.3 with the results appearing in [9], [21], [19] and [8], to get a complete answer to the local-global divisibility in products of elliptic curves defined over the rationals.

**Corollary 3.6.** *Let  $g$  be a positive integer and let  $\mathcal{E}_1, \mathcal{E}_2, \dots, \mathcal{E}_g$  be elliptic curves defined over  $\mathbb{Q}$  with Weierstrass form respectively  $y^2 = x^3 + b_i x + c_i$ , for  $i \in \{1, 2, \dots, g\}$ , where  $b_i, c_i \in \mathbb{Q}$ . Let  $p$  be a prime number. If  $p \geq 5$ , then the local-global divisibility by  $p^l$  holds in the product  $\mathcal{E}_1 \times \mathcal{E}_2 \dots \times \mathcal{E}_g$  over  $\mathbb{Q}$ , for every positive integer  $l$ . If  $p \in \{2, 3\}$ , then the local-global divisibility by  $p^l$  holds in the product  $\mathcal{E}_1 \times \mathcal{E}_2 \dots \times \mathcal{E}_g$  over  $\mathbb{Q}$  only when  $l = 1$ ; on the contrary, when  $l \geq 2$ , there are counterexamples.*

**Remark 3.7. Counterexamples.** For powers of 2 (resp. powers of 3), the explicit counterexamples to the local-global divisibility appearing in [18] and [19] give also explicit counterexamples to the local-global divisibility by  $2^l$  (resp.  $3^l$ ), for every  $l \geq 2$ , in products of elliptic curves defined over  $\mathbb{Q}$  (resp. over the cyclotomic field  $\mathbb{Q}(\zeta_3)$ ), for all  $g$ . It suffices to take the product of elliptic curves  $\mathcal{E}_1, \dots, \mathcal{E}_g$  with at least one of the  $\mathcal{E}_i$ 's being a curve giving a counterexample.

## 4 Proof of Theorem 1.4

First note that if  $\dim(A) = 2^h$ , then  $\text{Gal}(k(\mathcal{A}[p])/k)$  is isomorphic to a subgroup of  $\text{GL}_{2^{h+1}}(p)$ . As above, to ease notation we set  $n = 2^{h+1}$ , so that we can simply refer to  $\text{GL}_n(p)$  and, more generally, to  $\text{GL}_n(p^m)$ ,  $m \geq 1$ .

Our assumption that  $G$  is isomorphic to a subgroup of  $\text{GL}_{2^{h+1}}(p^m)$  (instead of simply  $\text{GL}_{2^{h+1}}(p)$ ) is just a technical one, since dealing with powers of  $p$  in lieu of  $p$  will be useful when  $G$  is of type  $\mathcal{C}_3$  (and it is isomorphic to a subgroup of  $\text{GL}_t(p^r).C_r$ , with  $n = tr$  and  $r$  prime) or  $G$  is of type  $\mathcal{C}_5$  (and it is isomorphic to a subgroup of  $\text{GL}_n(p^r)$ , with  $r$  a prime dividing  $m$ ).

For  $h = 0$  and  $G < \mathrm{GL}_2(p^m)$ , the following statement can be deduced from the proof of [11, Theorem 1] and from Remark 3.2.

**Lemma 4.1.** *Let  $k$  be a number field that does not contain  $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ . Let  $\mathcal{A}$  be an algebraic group defined over  $k$ , such that  $\mathrm{Gal}(k(\mathcal{A}[p^l])/k) \lesssim \mathrm{GL}_2(p^m)$ , where  $p > 3$  is a prime number and  $l, m$  are positive integers. If  $\mathcal{A}[p^l]$  is either an irreducible or a decomposable  $G_k$ -module, then the local-global principle holds for divisibility by  $p^l$  in  $\mathcal{A}$  over  $k$ .*

In particular that result holds when  $l = m = 1$ . From now on, we may assume that  $h \geq 1$  (i. e.  $\dim(A) \geq 2$  and  $n \geq 4$ ). Let  $G$  be a subgroup of  $\mathrm{GL}_n(p^m)$  and let  $\tilde{G} := G \cap \mathrm{SL}_n(p^m)$ . Since  $|\mathrm{GL}_n(p^m)| = (p^m - 1)|\mathrm{SL}_n(p^m)|$ , then the  $p$ -Sylow subgroup of  $\mathrm{GL}_n(p^m)$  coincides with the  $p$ -Sylow subgroup of  $\mathrm{SL}_n(p^m)$ . By Lemma 2.2, we have  $H_{\mathrm{loc}}^1(G, \mathcal{A}[p^m]) = 0$  if and only if  $H_{\mathrm{loc}}^1(\tilde{G}, \mathcal{A}[p^m]) = 0$ . Therefore we may assume  $G \leq \mathrm{SL}_n(p^m)$ . If  $G = \mathrm{SL}_n(p^m)$ , then, being  $n = 2^{h+1}$  and  $p \neq 2$ , the nontrivial scalar matrix  $-I$  belongs to  $\mathcal{A}$ . By Corollary 2.4 we get the triviality of  $H_{\mathrm{loc}}^1(G, \mathcal{A}[p^m])$ . From now on we will assume, without loss of generality, that  $G$  is a proper subgroup of  $\mathrm{SL}_n(p^m)$ .

For  $h = 1$  we give a proof of Theorem 1.4 based on a case by case analysis of the possible maximal subgroups of  $\mathrm{SL}_4(p^m)$ . Then we prove the statement for a general  $h$ , using the classification of the possible maximal subgroups of  $\mathrm{SL}_n(q)$  resumed in Table 1, combined with induction for some of the classes  $\mathcal{C}_i$  of groups. By the proof it will be clear that for subgroups of geometric type  $\mathcal{C}_i$ , with  $i \neq 6$ , everything works for every  $p > 3$  too. The class  $\mathcal{C}_6$  is the hardest to be described explicitly between the ones of geometric type. Because of the groups  $G$  in that class we possibly have to choose  $p_h \neq 3$ , for  $h \geq 3$ . Furthermore, for  $h \geq 3$  a complete classification of the subgroups of type  $\mathcal{C}_9$  is unknown, then for such integers we cannot show an explicit  $p_h$ , even if we can prove its existence. In the very last part of the proof, looking at the maximal subgroups of  $\mathrm{SL}_8(p^m)$ , we establish an explicit  $p_2$ .

#### 4.1 The case of abelian varieties of dimension 2

In this subsection we prove Theorem 1.4 for abelian varieties of dimension 2. Assume that  $\mathrm{Gal}(k(\mathcal{A}[p^l])/k)$  is isomorphic to a proper subgroup of  $\mathrm{SL}_4(p^m)$ , for any positive integer  $m$ . First of all, we recall some notation and some group isomorphisms.

**Notation 3.** Let  $s$  be a positive integer. The extraspecial 2-group of *minus type*  $2_-^{1+2s}$  is a central product of a quaternion group of order 8 with one or more dihedral groups

of order 8 (see for instance [14]). The extraspecial 2-group of *plus type*  $2_+^{1+2s}$  is a central product of dihedral groups of order 8. The *symplectic type* is given by a central product of either type of extraspecial 2-groups with a cyclic group of order 4.

**Lemma 4.2** ([3], Proposition 1.10.1). *The following isomorphisms hold*

- 1)  $\mathrm{SO}_4^+(q) \cong \mathrm{SL}_2(q) \times \mathrm{SL}_2(q)$ ;
- 2)  $\mathrm{SO}_4^-(q) \cong \mathrm{SL}_2(q^2)$ .

We also recall the classification of the maximal subgroups of  $\mathrm{SL}_4(p^m)$  and the classification of the maximal subgroups of the symplectic group  $\mathrm{Sp}_4(q)$  (when  $q$  is odd) appearing in [3].

**Lemma 4.3.** *Let  $q = p^m$ , where  $p$  is an odd prime and  $m$  is a positive integer. Let  $d := \gcd(q - 1, 4)$ . The maximal subgroups of  $\mathrm{SL}_4(q)$  are*

- (a) *a group of type  $\mathcal{C}_1$ , the stabilizer of a projective point, i. e. the group  $C_q^3 : \mathrm{GL}_3(q)$ , having order  $q^6(q^3 - 1)(q^2 - 1)(q - 1)$ ;*
- (b) *a group of type  $\mathcal{C}_1$ , the stabilizer of a projective line, having order  $q^4|\mathrm{SL}_4(q)|^2(q - 1) = q^6(q^2 - 1)^2(q - 1)$ ;*
- (c) *a group of type  $\mathcal{C}_1$ , the stabilizer of two distinct projective points and a projective line, having order  $q^5|\mathrm{GL}_2(q)|(q - 1) = q^6(q^2 - 1)(q - 1)^3$ ;*
- (d) *a group of type  $\mathcal{C}_1$ , a group isomorphic to  $\mathrm{GL}_3(q)$ , that stabilizes both a projective point and a projective plane, whose direct sum is  $\mathbb{F}_q^4$ , having order  $q^3(q^3 - 1)(q^2 - 1)(q - 1)$ ;*
- (e) *a group of type  $\mathcal{C}_2$ , the stabilizer of a decomposition of four subspaces of dimension 1 whose direct sum is  $\mathbb{F}_q^4$ , i. e. a group of order  $(q - 1)^3 4!$ ;*
- (f) *a group of type  $\mathcal{C}_2$ , the stabilizer of a decomposition of two subspaces of dimension 2 whose direct sum is  $\mathbb{F}_q^4$ , i. e. a group of order  $2|\mathrm{SL}_2(q^2)|(q - 1) = 2q^2(q^2 - 1)^2(q - 1)$ ;*
- (g) *a group of type  $\mathcal{C}_3$ , a group of order  $2q^2(q^4 - 1)(q + 1)$ , which has  $\mathrm{SL}_2(q^2)$  as a normal subgroup;*
- (h) *a group of type  $\mathcal{C}_6$ , the group  $C_4 \circ 2^{1+4} \cdot S_6$ ;*

- (i) a group of type  $C_6$ , the group  $C_4 \circ 2^{1+4} \cdot A_6$ ;
- (j) a group of type  $C_8$ , a group of order  $d|\mathrm{SO}_4^+(q)|$ , which has  $\mathrm{SO}_4^+(q)$  as a normal subgroup;
- (k) a group of type  $C_8$ , a group of order  $d|\mathrm{SO}_4^-(q)|$ , which has  $\mathrm{SO}_4^-(q)$  as a normal subgroup;
- (l) a group of type  $C_8$ , the group  $\mathrm{Sp}_4(q) \cdot C_2$  of order  $2q^4(q-1)(q^2-1)(q^4-1)$ ;
- (m) a group of type  $C_9$ , the group  $A_7$  (only if  $p = 2$ );
- (n) a group of type  $C_9$ , the group  $C_d \circ C_2 \cdot \mathrm{SL}_2(7)$ ;
- (o) a group of type  $C_9$ , the group  $C_d \circ C_2 \cdot A_7$ ;
- (p) a group of type  $C_9$ , the group  $C_d \circ C_2 \cdot U_4(2)$ .

**Lemma 4.4.** *Let  $q = p^m$ , where  $p$  is an odd prime and  $m$  is a positive integer. The maximal subgroups of  $\mathrm{Sp}_4(q)$  are*

- (1.1) a group of type  $C_1$ , the group  $E_q \cdot E_q^2 : ((q-1) \times \mathrm{Sp}_2(q))$ , of order  $q^4(q-1)^2$ ;
- (1.2) a group of type  $C_1$ , the group  $E_q^3 : \mathrm{GL}_3(q)$ , of order  $q(q^3-1)(q^2-1)(q-1)$ ;
- (1.3) a group of type  $C_2$ , the stabilizer of a decomposition of two subspace of dimension 2 whose direct sum is  $\mathbb{F}_q^4$ , i. e.  $\mathrm{Sp}_2(q)^2 \rtimes C_2$ ;
- (1.4) a group of type  $C_2$ , the group  $\mathrm{GL}_2(q) \cdot C_2$ ;
- (1.5) a group of type  $C_3$ , the group  $\mathrm{Sp}_2(q^2) \rtimes C_2$ ;
- (1.6) a group of type  $C_6$ , the group  $2_-^{1+4} \cdot S_5$ ;
- (1.7) a group of type  $C_6$ , the group  $2_-^{1+4} \cdot A_5$ ;
- (1.8) a group of type  $C_9$ , the group  $C_2 \cdot A_6$ ;
- (1.9) a group of type  $C_9$ , the group  $C_2 \cdot S_6$ ;
- (1.10) a group of type  $C_9$ , the group  $C_2 \cdot A_7$  (only for  $p = 7$ );
- (1.11) a group of type  $C_9$ , the group  $\mathrm{SL}_2(q)$ .

**Proof of Theorem 1.4 for  $h=1$ .** Let  $p > 3$ . Without loss of generality we assume that  $G$  is contained in a proper subgroup of  $\mathrm{SL}_4(q)$ , where  $q = p^l$ , and we use Lemma 4.7. We furthermore assume that  $\mathcal{A}[p^l]$  is either an irreducible or a decomposable  $G$ -module. In particular we are not in one of the cases (a), (b), (c), unless we can apply Remark 3.2 and, because of Lemma 4.1, to get the vanishing of  $H_{\mathrm{loc}}^1(G_p, \mathcal{A}[p^l])$ .

If we are in case (d), then  $G$  is of type  $C_1$ , but acts decomposably on  $\mathcal{A}[p^l]$ . Thus  $H_{\mathrm{loc}}^1(G_p, \mathcal{A}[p^l]) = 0$ , by Remark 3.2 and Lemma 4.1 again.

If we are in cases (e), then  $p \nmid |G|$ , the  $p$ -Sylow subgroup of  $G$  is trivial and  $H_{\mathrm{loc}}^1(G, \mathcal{A}[p^l]) = 0$ .

In case (f), the  $p$ -Sylow subgroup  $G_p$  of  $G$  has shape

$$\begin{pmatrix} 1 & a & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & b \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

where  $a, b \in \mathbb{Z}/p\mathbb{Z}$ . By Lemma 4.1 and Remark 3.2, the first local cohomology group  $H_{\mathrm{loc}}^1(G_p, \mathcal{A}[p^l])$  is trivial. Thus  $H_{\mathrm{loc}}^1(G, \mathcal{A}[p^l]) = 0$ .

In case (g), we have that  $G$  is contained in a group that has a normal subgroup isomorphic to  $\mathrm{SL}_2(p^2)$ , with index not divisible by  $p$ . Observe that the  $p$ -Sylow subgroup  $G_p$  of  $G$  is contained in  $G' := \mathrm{SL}_2(p^2) \cap G$ . We use Lemma 4.1 to get  $H_{\mathrm{loc}}^1(G_p, \mathcal{A}[p^l]) = 0$ , that is equivalent to  $H_{\mathrm{loc}}^1(G, \mathcal{A}[p^l]) = 0$ .

If we are in case (h) (resp. case (i)) and  $p > 5$ , then the  $p$ -Sylow subgroup of  $G$  is trivial too and  $H_{\mathrm{loc}}^1(G, \mathcal{A}[p^l]) = 0$ . If we are in case (h) (resp. case (i)) and  $p = 5$ , then the 5-Sylow subgroup of  $G$  is cyclic and  $H_{\mathrm{loc}}^1(G, \mathcal{A}[p^l]) = 0$ .

In cases (j) and (k) we use the group isomorphisms listed in Lemma 4.2. Then both cases are covered by Lemma 4.1.

Consider case (l), i. e.  $G$  is isomorphic to a subgroup of  $\mathrm{Sp}_4(p^m).C_2$ . Since  $p \neq 2$ , then  $G_p$  is contained in  $\mathrm{Sp}_4(p^m)$ . To ease notation, without loss of generality, we may assume  $G \lesssim \mathrm{Sp}_4(p^m)$ . If  $G = \mathrm{Sp}_4(p^m)$ , then  $-I_4 \in G$ . Since  $p \neq 2$ , then  $G$  contains a nontrivial scalar matrix and, by Corollary 2.4, we have  $H_{\mathrm{loc}}^1(G, \mathcal{A}[p^l]) = 0$ . If  $G = \langle I_4 \rangle$ , then  $H_{\mathrm{loc}}^1(G, \mathcal{A}[p^l])$  is trivial too. Therefore, we assume that  $G$  is a proper subgroup of  $\mathrm{Sp}_4(p^m)$  and we use Lemma 4.4.

In cases (1.1) and (1.2), the group  $G$  acts reducibly over  $\mathcal{A}[p^l]$ .

In cases (1.3) and (1.4), the group  $G_p$  acts decomposably over  $\mathcal{A}[p^l]$  and  $H_{\mathrm{loc}}^1(G, \mathcal{A}[p^l]) = 0$ , by Remark 3.2 and Lemma 2.2.

Consider case **(1.5)**. Then  $G_p$  is isomorphic to a subgroup of the  $p$ -Sylow subgroup of  $\mathrm{Sp}_2(p^{2m})$ . In particular  $G_p$  is isomorphic to a subgroup of  $\mathrm{SL}_2(p^{2m})$ . By Lemma 4.1, we get  $H_{\mathrm{loc}}^1(G_p, \mathcal{A}[p^l]) = H_{\mathrm{loc}}^1(G, \mathcal{A}[p^l]) = 0$ .

In cases **(1.6)** and **(1.7)**, if  $p > 5$ , then  $p \nmid |G|$ , implying  $H_{\mathrm{loc}}^1(G, \mathcal{A}[p^l]) = 0$ . If  $p = 5$ , we have that the 5-Sylow subgroup of  $G$  is cyclic and  $H_{\mathrm{loc}}^1(G, \mathcal{A}[p^l]) = 0$  too.

In cases **(1.8)**, **(1.9)** and **(1.10)**, the  $p$ -Sylow subgroup of  $G$  is either trivial or cyclic, for all  $p > 3$ .

Case **(1.11)** is covered by Lemma 4.1 again.

We are left with the cases when  $G$  is of type  $\mathcal{C}_9$  and it is not contained in  $\mathrm{Sp}_4(p)$ . In all those cases **(m)**, **(n)**, **(o)** and **(p)** the  $p$ -Sylow subgroup  $G_p$  of  $G$  is either trivial or cyclic, for all  $p > 3$ . Then  $H_{\mathrm{loc}}^1(G, \mathcal{A}[p^l]) = 0$ .  $\square$

**Remark 4.5.** From the proof, it is clear that the conclusion holds not only for abelian varieties of dimension 2, but even for all algebraic groups  $\mathcal{A}$  such that  $\mathcal{A}[p] \simeq (\mathbb{Z}/p^l\mathbb{Z})^4$  and  $\mathrm{Gal}(k(\mathcal{A}[p^l])/k) \lesssim \mathrm{GL}_4(p^m)$ , with  $m \geq 1$ .

## 4.2 General Case

We are going to prove Theorem 1.4, for the general case of an abelian variety of dimension  $2^h$ , that corresponds to the proof of the following proposition. We will prove  $p_2 = 3$  in next subsection.

**Proposition 4.6.** *Let  $p$  be a prime number and let  $l, h$  be positive integers. Let  $k$  be a number field that does not contain  $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ . Let  $\mathcal{A}$  be an abelian variety defined over  $k$ , of dimension  $2^h$ , where  $h \geq 0$ . Let  $n = 2^{h+1}$  and assume that  $\mathrm{Gal}(k(\mathcal{A}[p^l])/k)$  is isomorphic to a subgroup of  $\mathrm{GL}_n(p^m)$ , for some positive integer  $m$ . For every  $h$ , there exists a prime  $p_h$ , depending only on  $h$ , such that if  $p > p_h$  and the local-global divisibility by  $p$  fails in  $\mathcal{A}(k)$ , then  $\mathrm{Gal}(k(\mathcal{A}[p^l])/k)$  acts reducibly but not decomposably over  $\mathcal{A}[p^l]$ .*

*Proof.* Let  $p > 3$  and, as above, let  $n = 2^h$ . Suppose that  $G$  acts either irreducibly or decomposably on  $\mathcal{A}[q]$ , where  $q = p^l$ . We use the description of the subgroups of  $\mathrm{GL}_n(q)$  of geometric type given in Table 1. For some classes of groups we proceed by induction, having already proved the statement for  $h \in \{0, 1\}$ . Thus, assume that the proposition holds for all integers  $h' < h$ . We will prove it for  $h$ .

Because of our assumptions, the group  $G$  is not of class  $\mathcal{C}_1$ , unless its action on  $\mathcal{A}[q]$  is decomposable. For all  $p > p_{h-1}$ , the triviality of  $H_{\mathrm{loc}}^1(G, \mathcal{A}[q])$  follows from Remark



3.2 and induction.

Suppose that  $G$  is of type  $\mathcal{C}_2$ . Then  $G$  is the wreath product of a group  $G'$  of matrices with  $2^\alpha$  diagonal blocks by a symmetric group  $S_{2^\alpha}$ , where  $\alpha \leq h$ . Since  $p > 2$ , then the  $p$ -Sylow subgroup  $G_p$  of  $G$  is contained in  $G'$ . Thus, by Remark 3.2 and by induction, we get  $H_{\text{loc}}^1(G_p, \mathcal{A}[p^l]) = 0$ , for all  $p > p_{h-1}$ . Consequently  $H_{\text{loc}}^1(G, \mathcal{A}[p^l]) = 0$ , for all  $p > p_{h-1}$ , because of Lemma 2.2.

Suppose now that  $G$  is of type  $\mathcal{C}_3$ . Then  $G$  is isomorphic to a subgroup of  $\text{GL}_t(p^{mr}) \cdot C_r$ , where  $r$  is a prime and  $n = tr$ . Since  $n = 2^{h+1}$ , then  $r = 2$  and  $t = 2^h$ . Furthermore  $p$  does not divide  $r$  and we may assume without loss of generality that  $G$  is isomorphic to a subgroup of  $\text{GL}_t(p^{mr})$ . Since  $t|n$ ,  $t \neq n$ , we use induction to get  $H_{\text{loc}}^1(G, \mathcal{A}[p^l]) = 0$ , for every  $p > p_{h-1}$ .

Suppose that  $G$  is of type  $\mathcal{C}_4$ . Then  $G$  is isomorphic to a subgroup of a central product  $\text{GL}_t(p^m) \circ \text{GL}_r(p^m)$  acting on a tensor product  $V_1 \otimes V_2 = \mathcal{A}[p^l]$ , where  $rt = n = 2^h$  and  $V_1, V_2$  are vectorial spaces over  $\mathbb{F}_{p^m}$ , with dimension respectively  $t$  and  $r$ . A central product  $\Gamma$  of two groups is a quotient of their direct product by a subgroup of its center. Then every subgroup of  $\Gamma$  is a central product too. So let  $G = G_t \circ G_r$ , with  $G_t$  acting on  $V_1$  and  $G_r$  acting on  $V_2$ . Consider  $Z_{\sigma \otimes \tau}$ , with  $\sigma \otimes \tau \in G_t \circ G_r$ , representing a cocycle of  $G$  with values in  $\mathcal{A}[p^l] = V_1 \otimes V_2$ . If  $Z_{\sigma \otimes \tau}$  satisfies the local conditions, then there exists  $A_{\sigma \otimes \tau} \in V_1 \otimes V_2$  such that  $Z_{\sigma \otimes \tau} = (\sigma \otimes \tau - 1 \otimes 1)A_{\sigma \otimes \tau}$ , for all  $\sigma \otimes \tau \in G_t \circ G_r$ . Observe that  $A_{\sigma \otimes \tau} = A_{\sigma \otimes \tau, 1} \otimes A_{\sigma \otimes \tau, 2}$ , for some  $A_{\sigma \otimes \tau, 1} \in V_1$  and  $A_{\sigma \otimes \tau, 2} \in V_2$ . We have two separated actions of  $G_t$  on  $V_1$  and  $G_r$  on  $V_2$ . Then we can construct a cocycle  $Z_\sigma := (\sigma - 1)A_\sigma$ , with  $\sigma \in G_t$ , by choosing  $A_\sigma$  among the possible  $A_{\sigma \otimes \tau, 1} \in V_1$ . In the same way we can construct a cocycle  $Z_\tau := (\tau - 1)A_\tau$ , with  $\tau \in G_r$ , by choosing  $A_\tau$  among the possible  $A_{\sigma \otimes \tau, 2} \in V_2$ . For the tensor product construction, a priori we could have more than one choice of  $A_\sigma$  (respectively  $A_\tau$ ) for each  $\sigma$  (resp.  $\tau$ ). Anyway, we choose just one  $A_\sigma$  (resp.  $A_\tau$ ). We will have no problems about this choice, because of the two separated actions of  $G_t$  and  $G_r$  respectively on  $V_1$  and  $V_2$ . Observe that even in the general case of Definition 2.1, when a cocycle satisfies the local conditions, there could exist various  $A_\sigma$  giving the equality  $Z_\sigma = (\sigma - 1)A_\sigma$ . Anyway we make just one choice for  $A_\sigma \in \mathcal{A}[q]$ , for each  $\sigma \in G$ . Since  $r = 2^\alpha$ , with  $\alpha < h$ , by induction  $H_{\text{loc}}^1(G_r, V_1) = 0$ , for every  $p > p_\alpha$ , unless  $G_r$  acts reducibly but not decomposably over  $V_1$ . Observe that if  $G_r$  acts reducibly over  $V_1$ , then also  $G_r \otimes G_t$  is a parabolic group and  $G$  acts reducibly over  $\mathcal{A}[p^l]$  too. That is a contradiction with our assumptions. Then  $H_{\text{loc}}^1(G_r, V_1) = 0$

and there exists  $A \in V_1$ , such that  $Z_\sigma = (\sigma - 1)A$ , for all  $\sigma \in G_r$ . In the same way, by induction, since  $t = 2^\beta$ , with  $\beta < h$  (and  $\beta + \alpha = h$ ), by induction, for all  $p > p_\beta$ , we have  $H_{\text{loc}}^1(G_t, V_2) = 0$ , unless  $G_t$  acts reducibly but not decomposably over  $V_2$ . As above, if  $G_t$  acts reducibly over  $V_2$ , then also  $G_r \otimes G_t$  is a parabolic group and  $G$  acts reducibly over  $\mathcal{A}[p^l]$  too. Since this contradicts our assumptions, then there exists  $B \in V_2$ , such that  $Z_\tau = (\tau - 1)B$ , for all  $\tau \in G_t$ . Therefore  $Z_{\sigma \otimes \tau} = (\sigma \otimes \tau - 1 \otimes 1)A \otimes B$ , for all  $\sigma \otimes \tau \in G_t \circ G_r$  and  $H_{\text{loc}}^1(G, \mathcal{A}[p^l]) = 0$ . Since  $2^h$  is the greatest proper divisor of  $n$ , then for every  $p > p_{h-1}$ , we have  $H_{\text{loc}}^1(G, \mathcal{A}[p^l]) = 0$ .

If  $G$  is of class  $\mathcal{C}_5$ , then  $G$  is isomorphic to a subgroup of  $\text{GL}_n(p^t)$ , where  $m = tr$ , with  $t$  a positive integer and  $r$  a prime. If  $G$  is the whole group  $\text{GL}_n(p^t)$ , then  $G$  contains  $-I$  and  $H_{\text{loc}}^1(G, \mathcal{A}[p^l]) = 0$ . If  $G$  is trivial, then  $H_{\text{loc}}^1(G, \mathcal{A}[p^l])$  is trivial too. Suppose that  $G$  is a proper subgroup of  $\text{GL}_n(p^t)$ . If  $G$  is still of class  $\mathcal{C}_5$ , then  $G$  is isomorphic to a subgroup of  $\text{GL}_n(p^{t_2})$ , for some integer  $t_2$ , such that  $t = r_2 t_2$ , with  $r_2$  prime. Again, if  $G = \text{GL}_n(p^{t_2})$ , then  $-I \in G$  and  $H_{\text{loc}}^1(G, \mathcal{A}[p^l]) = 0$  and we may assume that  $G$  is a proper subgroup of  $\text{GL}_n(p^{t_2})$ . And so on. Since  $m$  is finite and we are assuming that  $G$  is not trivial, then  $G$  is isomorphic to a subgroup of  $\text{GL}_n(p^{t_j})$  (for some positive integer  $t_j$  dividing  $m$ ) of class  $\mathcal{C}_i$ , with  $i \neq 5$ . We may then repeat the arguments used for other classes  $\mathcal{C}_i$ , with  $i \notin \{1, 5\}$ , to get  $H_{\text{loc}}^1(G, \mathcal{A}[p^l]) = 0$ .

Suppose that  $G$  is of class  $\mathcal{C}_6$ , i. e.  $G$  lies in the normalizer of an extraspecial group. This is possible only when  $m = 1$ , which is the case of main interest for us. When  $n = 2^h$ , we have the following possible types of maximal subgroups of class  $\mathcal{C}_6$  (see [14, §3.5]):  $E_{2^{2h}}.\text{Sp}_{2h}(2)$ ;  $2^{1+2h}.\mathcal{O}_{2h}^-(2)$ ;  $2^{1+2h}.\mathcal{O}_{2h}^+(2)$ . If  $p$  does not divide  $\prod_{i=1}^h (2^{2i} - 1)$ , then it does not divide neither  $|\text{Sp}_{2h}(2)|$ , nor  $|\mathcal{O}_{2h}^\epsilon(2)|$ , for every  $\epsilon \in \{+, -\}$ . Let  $p_{\bar{h}}$  be the greatest prime dividing  $\prod_{i=1}^h (2^{2i} - 1)$ . If  $p > p_{\bar{h}}$ , then  $H_{\text{loc}}^1(G, \mathcal{A}[p^l]) = 0$ .

Assume that  $G$  is of class  $\mathcal{C}_7$ . Thus  $G$  is the stabilizer of a tensor product decomposition  $\bigotimes_{i=1}^t V_r$ , with  $n = r^t$  and  $\dim(V_i) = r$ , for every  $1 \leq i \leq t$ . By using induction on  $t$  and the argument given in the case when  $G$  is of class  $\mathcal{C}_4$  as the base of the induction, we get  $H_{\text{loc}}^1(G, \mathcal{A}[p^l]) = 0$ , for every  $p > p_{h-1}$ .

Suppose that  $G$  is of class  $\mathcal{C}_8$ . Since  $p^m$  is odd and  $n = 2^h$  is even, then  $G$  is contained either in the group  $\text{Sp}_n(p^m)$ , or in a group  $\text{O}_n^\epsilon(p^m)$ , for any  $\epsilon \in \{+, -\}$ , or in the group  $U_n(p^{\frac{m}{2}})$ , with  $m$  even too. If  $G$  is one of the whole groups  $\text{Sp}_n(p^m)$  or  $\text{O}_n^\epsilon(p^m)$  or  $U_n(p^{\frac{m}{2}})$ , then it contains a scalar multiple of the identity and  $H_{\text{loc}}^1(G, \mathcal{A}[p^l]) = 0$ . Suppose that  $G$  is a proper subgroup of one of those three groups. From the classification of the maximal

subgroups of  $\mathrm{Sp}_n(p^m)$  and  $\mathrm{O}_n^\epsilon(p^m)$  and  $U_n(p^{\frac{m}{2}})$  (see [14], in particular Table 3.5B, Table 3.5C, Table 3.5D and Table 3.5E), we have that  $\mathrm{O}_n^\epsilon(p^m)$  and  $U_n(p^{\frac{m}{2}})$  do not contain groups of class  $\mathcal{C}_8$  and that the subgroups of  $\mathrm{Sp}_n(p^m)$  of class  $\mathcal{C}_8$  are  $\mathrm{O}_n^\epsilon(p^m)$  themselves, where  $\epsilon \in \{+, -\}$  (and  $n \geq 4$ ). Since we are assuming that  $G$  is strictly contained in one of those three groups, then it is a subgroup of class  $\mathcal{C}_i$ , for some  $i \neq 8$ . We get the conclusion by the same arguments used for those classes of groups.

For every  $n$ , there is a finite number of subgroups of  $\mathrm{GL}_n(p^m)$  of type  $\mathcal{C}_9$ . Unfortunately, as said above, for  $n \geq 12$  an explicit classification of those groups is not known. Anyway, there exists a prime  $p_{h'}$ , that is the greatest prime dividing the order of at least one of those subgroups of type  $\mathcal{C}_9$ . If  $G$  is of class  $\mathcal{C}_9$ , then  $H_{\mathrm{loc}}^1(G, \mathcal{A}[q]) = 0$ , for all  $p > p_{h'}$ .

Let  $p_h := \max\{p_{\bar{h}}, p_{h-1}, p_{h'}\}$ . Then  $H_{\mathrm{loc}}^1(G, \mathcal{A}[p^l]) = 0$ , for all  $p > p_h$ .  $\square$

### 4.3 The case of abelian varieties of dimension 4

To complete the proof of Theorem 1.4 (and consequently of Theorem 1.2, Corollary 1.3 and Theorem 1.5), we have to show  $p_2 = 3$ . By the proof of Proposition 4.6, it is clear that  $p_h$  depends only on  $p_{h-1}$  and on the subgroups of  $\mathrm{SL}_{2^{h+1}}(q)$  of class  $\mathcal{C}_6$  and of class  $\mathcal{C}_9$ . In the next lemma we recall the classification of the maximal subgroups of  $\mathrm{SL}_8(q)$  of those two classes (see [3]).

**Lemma 4.7.** *Let  $q = p^m$ , where  $p$  is an odd prime and  $m$  is a positive integer. Let  $d := \gcd(q-1, 4)$ . Let  $d := \gcd(q-1, 8)$ . The only maximal subgroup of  $\mathrm{SL}_8(q)$  of type  $\mathcal{C}_6$  is  $(C_d \circ 2^{1+6}) \cdot \mathrm{Sp}_6(2)$ . The maximal subgroups of  $\mathrm{SL}_8(q)$  of type  $\mathcal{C}_9$  are isomorphic to the following groups*

- (a)  $C_4 \cdot \mathrm{PSL}_3(4)$ , for  $q = p = 5$ ;
- (b)  $C_d \circ C_4 \cdot \mathrm{PSL}_3(4)$ , for  $q = p \equiv 9, 21, 29, 41, 61, 69 \pmod{80}$ ;
- (c)  $C_8 \circ C_4 \cdot \mathrm{PSL}_3(4).C_2$ , for  $q = p \equiv 1, 49 \pmod{80}$ ;
- (d)  $C_8 \circ C_4 \cdot \mathrm{PSL}_3(4)$ , for  $q = p^2$ ,  $p \equiv \pm 3, \pm 13, \pm 27, \pm 37 \pmod{80}$ ;
- (e)  $C_8 \circ C_4 \cdot \mathrm{PSL}_3(4).C_2$ , for  $q = p^2$ ,  $p \equiv \pm 7, \pm 17, \pm 23, \pm 33 \pmod{80}$ .

**Proof of Theorem 1.3 for  $h = 2$ .** As noted above, by Theorem 1.4, if the group  $G$  lies in one of the classes  $\mathcal{C}_i$ , for  $i \notin \{1, 6, 9\}$ , then  $H_{\mathrm{loc}}^1(G, \mathcal{A}[p^l]) = 0$ , for all  $p > 3$ . Assume

that  $G$  is of class  $\mathcal{C}_6$ . By Lemma 4.7, we have that  $G$  is a subgroup of  $(C_d \circ 2^{1+6}) \cdot \mathrm{Sp}_6(2)$ , where  $d = \gcd(p^l - 1, 8)$ . Therefore the cardinality of  $|G|$  divides  $2^{19} \cdot 3 \cdot 7$ . For every prime  $p > 3$  the  $p$ -Sylow subgroup of  $G$  is either trivial or cyclic (this last case occurs only if  $p = 7$ ). In both cases  $H_{\mathrm{loc}}^1(G, \mathcal{A}[q]) = 0$ . If  $G$  is a group of class  $\mathcal{C}_9$ , then, by Lemma 4.7, the cardinality of  $G$  divides  $2^6 |\mathrm{PSL}_3(4)|$ . Since  $\mathrm{SL}_3(4)$  has a trivial center, then  $\mathrm{PSL}_3(4) = \mathrm{SL}_3(4)$  and the cardinality of  $G$  divides  $2^6 \cdot 3 \cdot 5 \cdot 7$ . Again, for all  $p > 3$  the  $p$ -Sylow subgroup of  $G$  is either trivial or cyclic (this last case occurs only if  $p = 5$  or  $p = 7$ ). We have  $H_{\mathrm{loc}}^1(G, \mathcal{A}[q]) = 0$ . Thus  $p_2 = 3$ .  $\square$

*Acknowledgments.* I am grateful to John van Bon, Roberto Dvornicich and Gabriele Ranieri for useful discussions. I wrote the last part of this paper at the Max Planck Institute for Mathematics in Bonn. I would like to thank all people there for their kind hospitality.

## References

- [1] ASCHBACHER, *On the maximal subgroups of the finite classical groups*, Invent. Math., **76** (1984), 469-514.
- [2] BAŠMAKOV M. I., *The cohomology of abelian varieties over a number field*, Russian Math. Surveys., **27** (1972) (English Translation), 25-70.
- [3] BRAY J. N., HOLT D. F., RONEY-DOUGAL C. M., *The maximal subgroups of the low-dimensional finite classical groups*, Cambridge University Press, Cambridge, 2013.
- [4] CASSELS J. W. S., *Arithmetic on curves of genus 1. III. The Tate-Šafarevič and Selmer groups.*, Proc. London Math. Soc., **12** (1962), 259-296.
- [5] CASSELS J. W. S., *Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung.*, J. reine angew. Math. **211** (1962), 95-112.
- [6] ÇIPERIANI M., STIX J., *Weil-Châtelet divisible elements in Tate-Shafarevich groups II: On a question of Cassels.*, J. Reine Angew. Math., **700** (2015), 175-207.
- [7] CREUTZ B., *Locally trivial torsors that are not Weil-Châtelet divisible*, Bull. London Math. Soc., **45** (2013), 935-942.

- [8] CREUTZ B., *On the local-global principle for divisibility in the cohomology of elliptic curve*, Math. Res. Lett., **23** no. 2 (2016), 377-387.
- [9] DVORNICICH R., ZANNIER U., *Local-global divisibility of rational points in some commutative algebraic groups*, Bull. Soc. Math. France, **129** (2001), 317-338.
- [10] DVORNICICH R., ZANNIER U., *An analogue for elliptic curves of the Grunwald-Wang example*, C. R. Acad. Sci. Paris, Ser. I **338** (2004), 47-50.
- [11] DVORNICICH R., ZANNIER U., *On local-global principle for the divisibility of a rational point by a positive integer*, Bull. Lon. Math. Soc., no. **39** (2007), 27-34.
- [12] HILTON P. J., STAMMBACH U., *A course in homological algebra*, GTM 4, Springer-Verlag, New York, 1971.
- [13] JENSEN C. U., LENZING H., *Model theoretic algebra, with particular emphasis on fields, rings, modules*, Algebra, Logic and Applications Series, vol. 2, Gordon and Breach Science Publishers, London, 1989.
- [14] KLEIDMAN P. B., LIEBECK M. W., *The subgroups structure of the finite classical groups*, London Math. Soc. Lecture Note Ser., 129, Cambridge University Press, Cambridge, 1990.
- [15] LANG S., *Elliptic curves: diophantine analysis*, Grundlehren der Mathematischen Wissenschaften 231, Springer, 1978.
- [16] MILNE J. S., *Abelian Varieties*, Arithmetic Geometry (Storrs, Conn., 1984), Springer, New York, 1986, 103-150.
- [17] PALADINO L., *Local-global divisibility by 4 in elliptic curves defined over  $\mathbb{Q}$* , Annali di Matematica Pura e Applicata, no. **189.1**, (2010), 17-23.
- [18] PALADINO L., *Elliptic curves with  $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$  and counterexamples to local-global divisibility by 9*, Le Journal de Théorie des Nombres de Bordeaux, Vol. **22**, n. 1 (2010), 138-160.
- [19] PALADINO L., *On counterexamples to local-global divisibility in commutative algebraic groups*, Acta Arithmetica, **148** no. 1, (2011), 21-29.
- [20] PALADINO L., RANIERI G., VIADA E., *On Local-Global Divisibility by  $p^n$  in elliptic curves*, Bulletin of the London Mathematical Society, **44** no. 5 (2012), 789-802.

- [21] PALADINO L., RANIERI G., VIADA E., *On minimal set for counterexamples to the local-global principle*, Journal of Algebra, **415** (2014), 290-304.
- [22] SANSUC J.-J., Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres. (French) [The Brauer group and arithmetic of linear algebraic groups on a number field], J. Reine Angew. Math. , **327** (1981), 12-80.
- [23] WONG S., *Power residues on abelian variety*, Manuscripta Math., no. **102** (2000), 129-137.

Laura Paladino

Max Planck Institute for Mathematics

Vivatgasse, 7

53111 Bonn

Germany

e-mail address: lpaladino@mpim-bonn.mpg.de